CLAIMS

What is claimed is:

Sub A1

1. A method of operation at a file server comprising:

accessing at said file server (i) information encrypted with a first encryption key and (ii) an entry from an access control list, said entry being associated with said encrypted information and a client authorized to read and modify said encrypted information, wherein said entry comprises a first decryption key encrypted with a second encryption key and wherein said first decryption key is usable to decrypt said encrypted information.

transmitting to said client said encrypted information and said entry.

2. The method of claim 1 further comprising prior to said accessing step:

storing said information encrypted with said first encryption key on said file server; and

storing said entry on said file server.

3. The method of claim 1 wherein said transmitting step comprises the step of transmitting said encrypted information and said entry in response to a request from said client.

4. The method of claim 1 wherein said transmitting step comprises the step of transmitting to said requesting client said access control list.

5. The method of claim 1 wherein said first encryption key and said first decryption key are symmetric.

ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

6. The method of claim 1 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and said first decryption key comprises the other of said public key and said private key of said first public/private key pair.

7. The method of claim 2 wherein said step of storing said entry on said file server includes the step of storing in association with said entry an unecrypted identifier associated with said client.

8. The method of claim 2 wherein said step of storing said entry on said file server comprises the step of storing an access control list, wherein said entry comprises one entry of a plurality of entries within said access control list, and said entry includes said first decryption key combined with a check value to form a data stream, wherein said data stream is encrypted with a second encryption key associated with said client; and

said transmitting step comprises the step of transmitting to said requesting client said encrypted information and said access control list.

9. The method of claim 8 wherein said check value comprises a value known to said client.

10. The method of claim 8 wherein said check comprises an identifier associated with said client.

ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

11. The method of claim 10 wherein said identifier comprises a client identifier that serves to identify said client;

12. The method of claim 8 wherein said identifier comprises a group identifier that identifies a group of which said client is a member.

13. A method for securely storing information on a file server and distributing the stored information, said method comprising:

encrypting information at one of a plurality of clients in communication with said file server, said information being encrypted with a first encryption key having an associated first decryption key;

encrypting said first decryption key with a second encryption key for each of said plurality of clients authorized to read and modify said information, wherein each respective one of said second encryption keys has a corresponding second decryption key retained by the respective one of said plurality of clients;

storing said encrypted information on said file server and storing on said file server said encrypted first decryption keys as a plurality of entries within an access control list, wherein each one of said entries is associated with one of said plurality of clients;

forwarding to at least a selected one of said plurality of clients said encrypted information and at least one of said entries;

decrypting said encrypted first decryption key contained in said at least one of said entries utilizing the

ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

second decryption key corresponding to the second encryption key for the respective entry; and

decrypting said encrypted information using said first decryption key to obtain said information.

14. The method of claim 13 wherein said forwarding step comprises the step of forwarding said encrypted information and said at least one of said entries to said selected one of said plurality of clients in response to a request received at said file server from said selected one of said plurality of clients.

15. The method of claim 14 wherein said request includes a client identifier associated with said selected one of said plurality of clients, said entries each include a client identifier associated with one of said plurality of clients, and wherein said forwarding step includes the step of forwarding to at least said selected one of said plurality of clients the said entry including the client identifier associated with the client identifier contained within said request.

16. The method of claim 13 wherein said forwarding step comprises the step of forwarding to said selected one of said plurality of clients said encrypted information and said access control list.

17. The method of claim 17 wherein said first encryption and decryption keys are symmetric.

18. The method of claim 13 wherein said second encryption and decryption keys are symmetric.

ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

19. The method of claim 13 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and the first decryption key comprises the other of said public key and said private key of said first public/private key pair.

20. A method for storing information securely on a file server for access by members of a group, said method comprising the steps of:

identifying the members of said group, wherein said group has a group identifier,

encrypting information with a first encryption key having an associated first decryption key;

encrypting said first decryption key with a group encryption key having an associated group decryption key for decrypting data encrypted with said group encryption key; and

storing said encrypted information on said file server and storing said encrypted first decryption key on said file server within an access control list associated with said encrypted information and containing, at least at some times, a plurality of encrypted first decryption keys.

21. A method for accessing information securely stored on a file server for access by members of a group, said method comprising:

identifying the members of said group, wherein said group has a group identifier,

encrypting information with a first encryption key having an associated first decryption key;

ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

encrypting said first decryption key with a group encryption key having an associated group decryption key for decrypting data encrypted with said group encryption key;

storing said encrypted information on said file server and storing said encrypted first decryption key on said file server within an access control list associated with said encrypted information and containing, at least at some times, a plurality of encrypted first decryption keys.

in response to a request received at said file server from one of said members of said group, forwarding to said one of said members of said group said encrypted information and at least said encrypted first decryption key encrypted with said group encryption key;

in a first decrypting step, decrypting said encrypted first decryption key with said group decryption key to obtain said first decryption key; and

in a second decrypting step, decrypting said encrypted information using said first decryption key to obtain said information.

22. The method of claim 21 wherein said method further includes the step of distributing said group decryption key to said members of said group and said first decrypting step comprises the step of decrypting the encrypted first decryption key by said one of said members of said group using the distributed group decryption key.

23. The method of claim 21 wherein said first decrypting step comprises the steps of:

forwarding said encrypted first decryption key to a group server associated with said group identifier;

ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

decrypting said encrypted first decryption key at said group server using said group decryption key; and

forwarding said first decryption key to said one of said group members.

24. The method of claim 23 wherein said step of forwarding said first decryption key to said one of said group members comprises the step of forwarding the first decryption key to said one of said group members over a secure channel.

25. The method of claim 24 wherein said secure channel is a physically secure channel.

26. The method of claim 24 wherein said secure channel comprises a non-secure communications path and said step of forwarding the first decryption key to said one of said group members over a secure channel comprises the steps of:

encrypting said first decryption key with a third encryption key having an associated third decryption key known to said one of said group members;

forwarding to said one of said group members said encrypted first decryption key encrypted with said third encryption key; and

decrypting by said one of said group members, said encrypted first decryption key encrypted with said third encryption key using said third decryption key.

27. The method of claim 26 wherein said third encryption key comprises a public key of a member public/private key pair and wherein said third decryption key comprises the member private key of said member public/private key pair.

ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

28. The method of claim 26 wherein said third encryption and decryption keys are symmetric.

29. The method of claim 21 wherein said first encryption and decryption keys are symmetric.

30. The method of claim 21 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and the first decryption key comprises the other of said public key and said private key of said first public/private key pair.

31. A method for accessing information stored securely on a file server

forwarding to said file server a request for information from a client;

in response to said request, receiving from said file server said information encrypted with a first encryption key having an associated first decryption key and at least one access control list entry associated with a client authorized to read and modify said information, said received at least one entry including said first decryption key encrypted with a second encryption key having an associated second decryption key;

decrypting said encrypted first decryption key using said second decryption key to obtain said first decryption key; and

decrypting said encrypted information using said first decryption key.

32. The method of claim 31 wherein said first encryption and decryption keys are symmetric.

ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

33. The method of claim 31 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and the first decryption key comprises the other of said public key and said private key of said first public/private key pair.

34. The method of claim 31 wherein said second encryption key comprises a public key of a member public/private key pair and said second decryption key comprises the private key of said member public/private key pair.

35. A computer program product including a computer readable medium, said computer readable medium having a file server computer program stored thereon, said file server computer program for execution in a computer and comprising:

program code for storing on said file server information encrypted with a first encryption key having a corresponding first decryption key;

program code for storing on said file server an access control list, said access control list including at least one entry, said at least one entry including said first decryption key encrypted with a second encryption key associated with one of a plurality of clients authorized to read and modify said information and having access to a second decryption key associated with said second encryption key; and

program code for transmitting to said one of said plurality of clients said encrypted information and said at least one entry.

ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

36. A computer data signal, said computer data signal including a computer program for use in accessing encrypted information stored on a file server, said computer program comprising:

program code for storing on said file server information encrypted with a first encryption key having a corresponding first decryption key;

program code for storing on said file server an access control list, said access control list including at least one entry, each of said at least one entry including said first decryption key encrypted with a second encryption key associated with one of a plurality of clients authorized to read and modify said information and having access to a second decryption key associated with said second encryption key; and

program code for transmitting to said one of said plurality of clients said encrypted information and said at least one entry.

37. Apparatus for accessing encrypted data stored on a file server comprising:

means for storing on said file server information encrypted with a first encryption key having a corresponding first decryption key;

means for storing on said file server an access control list, said access control list including at least one entry, said at least one entry including said first decryption key encrypted with a second encryption key associated with one of a plurality of clients authorized to read and modify said information and having access to a second decryption key associated with said second encryption key; and

ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

program code for transmitting to said one of said plurality of clients said encrypted information and said at least one entry.

5

ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313